



Guia de Personalizacion de Gnome

octubre 10th, 2010 ▶ Write comment

Hoy he tenido que reinstalar Ubuntu en mi portatil y ya sabeis que a veces necesita unos retoques y encuentre esta guia hecha por **Psifurius** (portallinux.wordpress.com)

[La Guia Extrema de Tuning Para Gnome4 2](#)

Si alguien quiere descargarlo tambien lo he subido a [Multiupload](#).



Linux



Write comment

Almacenamiento Redundante y Distribuido [RAID]

octubre 3rd, 2010 ▶ Write comment

BIENVENIDO

Bienvenido a MadHacking , ésta es una página dedicada al Auto-Aprendizaje [Informática , Seguridad , Programación , Mantenimiento , Redes ,etc] Espero que aprendas mucho visitando MadHacking. Att. MadPitbull_99

RECENT ENTRY

Guia de Personalizacion de Gnome

Almacenamiento Redundante y Distribuido [RAID]

Clusters de Servidores [Introduccion]

Conceptos basico de la Seguridad Informatica

Diseñando nuestro propio Sistema Operativo

CATEGORY

3D Max

Android

ASM

Bases de Datos

C / C++

C#

Corel Draw

Cracking | Ingeniería Inversa

CSS

Defacing

Diseño General

Diseño Web | General

Flash

Hacking General

HTML

Internet | General

Java

JavaScript

Juegos

ARCHIVES

octubre 2010

septiembre 2010

agosto 2010

julio 2010

junio 2010

mayo 2010

abril 2010

marzo 2010

febrero 2010

enero 2010

diciembre 2009

Los sistemas de almacenamiento RAID consisten en un conjunto de tecnicas hardware o software que utilizan varios discos para guardar la informacion. Este sistema de almacenamiento nos ayudara a garantizar algunos objetivos de la [Seguridad Informatica](#), como la disponibilidad .

Este sistema de almacenamiento distribuye o duplica la informacion entre los discos que lo componen de forma que se consiguen algunas mejoras:

- Mayor capacidad.
- Mayor tolerancia a fallos.
- Mayor velocidad.
- Mayor seguridad.

Tipos de RAID

RAID de Nivel 0 (RAID 0)

Los datos se distribuyen de forma equilibrada entre los 2 o mas discos del sistema de almacenamiento. Imaginemonos que tenemos una cancion y un sistema RAID 0, cuando el SO va a guardar esa cancion la parte en segmentos que suelen ser del mismo tamaño y los distribuye entre los dos discos duros, así una parte de la cancion estara en un disco duro y la otra en el otro disco duro. Esta tecnica favorece la velocidad pero hay que tener en cuenta que si uno de los dos discos duros falla la informacion es irrecuperable.

RAID de Nivel 1 (RAID 1)

Los datos de un disco se duplican en todos los demas. Los datos estan disponibles en dos o mas discos al mismo tiempo. Es conocido tambien como espejo, la cancion del ejemplo anterior ahora estara almacenada completamente (sin segmentarla) en todos los discos del RAID.

RAID de Nivel 5 (RAID 5)

Los datos se almacenan en varios discos y se guarda paridad de ellos. En la lectura se leen los datos solamente, el bloque de paridad es leido cuando hay un fallo. Es parecido a RAID 0 pero en uno de los discos se guarda la paridad. Imaginemonos el siguiente caso :

Disco 0	Disco 1	Disco 2	Disco 3 (paridad)
11011011	01101011	00011101	101


Los 1 y 0 son fragmentos de un fichero distribuido entre 3 discos y en el cuarto se guarda su paridad. Para calcular la paridad se cuenta el numero de 1, **si el numero de 1 es par entonces el primer dígito es 0 sino es 1**. Esquema : numero de 1 = par → 0 || numero de 1 = impar → 1

Implementacion

Se pueden implementar tanto por software (usando el sistema operativo) como por hardware (usando una controladora raid)

Links de controladoras raid : [Tarjeta Controladora RAID Dell](#) || [Tarjetas SCSI RAID](#)

 Seguridad Informatica

 Write comment

Clusters de Servidores [Introduccion]

octubre 2nd, 2010  Write comment



Un Cluster es un conjunto de varios ordenadores/servidores que trabajan como si fuera uno solo. Se unen mediante una red de alta velocidad, generalmente fibra optica, de forma que el conjunto se ve como uno un unico ordenador.

Linux

Mantenimiento PC

Noticias IT

Off Topic

Optimizacion Windows

Pascal | Delphi

Perl

Photoshop

PHP

Programación Vírca
(Malware)

Programacion | General

Python

Qt

Redes

Seguridad Informatica

Seguridad Wireless

Visual Basic

Webmaster / Scripts

WordPress

LINKS

0to255

Blog de Juan Carlos Andreu

ElHacker.Net

Hackin9

Lord RNA

RFC Editor

RFC Mini-Index

[A]ntrax [L]abs

WEBS AMIGAS:



WEB COMPARTE





Vista de un Cluster

Características:

- **Alta disponibilidad.** Siempre habrá un ordenador que ofrezca servicios, al menos que haya un corte de energía y todos estén apagados.

- **Alto rendimiento.** Las prestaciones de todos los equipos que componen el

cluster se suman.

- **Balanceo de carga.** Cuando un servidor está procesando demasiados datos comparte el procesamiento con otros servidores que componen su cluster y ellos le devuelven los datos procesados.

- **Escalabilidad.** Siempre debemos pensar en grande, podemos ampliar el número de equipos que componen nuestro cluster hasta el infinito. En 2003 Google contaba con más de 15000 ordenadores.

Clasificación de los Clusters:

- **De alto rendimiento,** ejecutan tareas que requieren una gran capacidad de cálculo o de grandes cantidades de memoria.
- **De alta disponibilidad,** se busca garantizar la disponibilidad de los servicios que ofrecen.
- **De alta eficiencia,** el objetivo principal es que puedan ejecutar el mayor número de tareas en el menor tiempo posible.

Componentes de los Clusters:

1. **Nodos,** es el nombre que recibe cualquier máquina que utilicemos para el Cluster. Pueden ser tanto ordenadores personales como servidores.
2. **Sistema Operativo,** debe tener 2 características básicas: multitarea y multiusuario.
3. **Conexión de Red,** es necesario conectar los nodos entre sí, se recomienda una red de alta prestaciones.
4. **Middleware,** es el software que gestiona el cluster, su objetivo es que el usuario del cluster tenga la sensación de estar frente a un único superordenador ya que provee una interfaz única de acceso al sistema.
5. **Sistema de Almacenamiento,** podemos hacer uso del sistema de almacenamiento interno de los equipos o de uno externo, como NAS o SAN (explicados más abajo)

Sistemas de almacenamiento externo:

- **NAS,** los discos de almacenamiento están conectados al servidor y se accede a ellos mediante los protocolos de red TCP/IP. Cuando se pide un dato, el cliente se lo pide al servidor, el servidor accede al disco duro y se lo pasa al usuario.
- **SAN,** también conocidos como discos duros en red. Disponen de los protocolos TCP/IP y se pueden configurar para conectarlos a una red y acceder a ellos como si se tratara de un equipo. Suelen estar conectados con redes de alta velocidad (fibra óptica).

Con este artículo quería acercar al usuario novato a la tecnología de los clusters. Si tenéis ganas y los recursos necesarios os podéis montar en vuestra casa un mini-cluster. Podéis elegir entre varios sistemas operativos: Windows Server, Solaris, FreeBSD, AIX, OpenMosix, etc.

Más Información:

[_ Wikipedia](#)

[_ Como montar un cluster \[mini-guia\]](#)

Intentare hacer una pequeña introducción a la Seguridad Informática explicando los conceptos básicos que se debe saber antes de adentrarnos en más teoría para personas que tienen unos conocimientos básicos de Seguridad Informática o Hacking.

Objetivos de la Seguridad Informática

La mayoría de estos conceptos están definidos en el estándar [ISO27002](#) . Los objetivos de la SI (Seguridad Informática, lo llamaremos así) son los siguientes:

- **Confidencialidad** : Asegura que el acceso a la información está adecuadamente autorizado. Consiste en la capacidad de garantizar que la información, almacenada en los sistemas informáticos o que circula por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir si esa información cayera en manos ajenas, estas no podrían interpretarla ni acceder a su contenido.
- **Integridad** : Como su nombre bien dice, asegura la integridad de la información (que no haya datos corruptos, que la información no haya sido alterada/modificada, etc).
- **Disponibilidad** : Garantiza el acceso a la Información o mejor dicho garantiza que los usuarios autorizados pueden acceder a la información cuando la necesitan. Dicho de mejor forma, es garantizar que tanto los sistemas informáticos como los datos van a estar disponibles a los usuarios que los necesitan en todo momento.
- **No Repudio** : Este objetivo muchos libros de SI no lo reconocen ni lo mencionan, pero es un factor bastante importante. Garantiza que ninguno de los dos, emisor y receptor, hayan recibido o transmitido un mensaje.

Ahora vamos a ver cómo asegurar estos objetivos :

1. Autenticación, permite identificar al emisor de un mensaje, al creador de un documento o a la persona que se conecta a una red o un servicio.
2. Autorización, controla el acceso de los usuarios a una determinada zona después de haberse identificado correctamente.
3. Auditoría, verifica el correcto funcionamiento de las políticas o medidas de seguridad ya implementadas.
4. Encriptación, ayuda que la información transmitida no puede ser interpretada por cualquier persona sin que tenga el algoritmo de descifrado o clave.
5. Copias de Seguridad o Backups, en caso de fallos podemos recuperar rápidamente la información perdida y garantizar la disponibilidad.
6. Antivirus y programas de protección, garantiza la protección de los equipos para la mayoría del malware.
7. Cortafuegos o Firewall, registra los intentos de conexión no deseados, en ambos sentidos, desde los equipos hacia la red y viceversa.
8. Servidores Proxy, hacen de intermediarios entre una red interna (corporativa) y una externa (Internet). Auditan y autorizan el acceso a servicios, recursos, páginas web, etc.
9. Firma electrónica o certificado digital, este mecanismo nos ayuda a garantizar la Integridad y el No Repudio.
10. Leyes para la protección de datos personales.
11. Claramente hay muchos más, esto se podría convertir en una lista interminable, estos ejemplos nos pueden dar una idea.

Clasificación de la Seguridad

Clasificación de la Seguridad en función del recurso protegido

- **Física**, es aquella que trata de proteger el hardware, desastres naturales, terremotos, inundaciones, sobrecargas eléctricas.
- **Lógica**, complementa a la seguridad Física, protegiendo el software de los equipos informáticos, por ejemplo : pérdida de datos, intrusiones, infecciones con Malware, etc.

Clasificación de la Seguridad en función de las medidas oportunas

- **Activa**, intenta prevenir los problemas. Uso de contraseñas, controles de acceso, software de seguridad, firmas y certificados digitales, sistemas de almacenamiento con tolerancia a fallos, etc.
- **Pasiva**, intenta minimizar los daños/perdidas una vez ocurridos. SAI, discos redundantes, etc.

Actuaciones para mejorar la Seguridad

- Identificar los activos (los objetos que la empresa quiere proteger).
- Formacion de los trabajadores en cuanto a materias de seguridad.
- Evaluar los riesgos, considerando el impacto que pueden tener los daños.
- Diseñar el plan de actuaciones : Seguridad Pasiva y Activa.

Tipos de Vulnerabilidades y su calificacion

1. Sobre aplicaciones o sistemas.
2. Sobre aplicaciones no instaladas.
3. No conocidas.

Clasificacion:

Calificacion	Definicion
Critica	Vulnerabilidad que puede permitir la propagacion de un gusano de Internet sin la accion del usuario
Importante	Puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuracion predeterminadas, auditorias o la dificultad de explotar una vulnerabilidad
Baja	Vulnerabilidad muy dificil de explotar o cuyo impacto es minimo

Tipos de Vulnerabilidades:

1. **Interupcion**, un recurso del sistema o de la red deja de estar disponible debido a un ataque.Ejemplo : Denegacion de Servicios (DoS), .
2. **Intercepcion**, un intruso accede a la informacion de nuestro equipo o a la que enviamos por la red. Ejemplo : Sniffing, malware, keylogger, troyanos, etc.
3. **Modificacion**, la informacion ha sido modificada sin autorizacion, por lo que ya no es valida (Integridad). Ejemplo : malware.
4. **Falsificacion/Fabricacion**, se crea un producto (por ejemplo una pagina Web) dificil de distinguir del autentico y que puede utilizarse para hacerse con informacion confidencial de usuario.Ejemplo : Spoofing, Phising.

Mediante este pequeño artículo quería dar una introducción a los conceptos básicos de la Seguridad Informática.

